

IF YOU SUSPECT IT, REPORT IT

If you receive a suspicious message urging you to share information, download a file or click on a link, report it!

Cyberattacks can appear in numerous ways: email, SMS, instant message, call..., so don't let your guard down.

Today 9:03



Urgent! Action required

Dear Customer, confirm your password now, or we'll close your account in the next 24h.

www.confirmationsecureaccess.com/b/6mn

Smishing example

Have you received a suspicious communication?

Pretending to be Santander

Please let us know.

Remember, Santander will never ask you for your full passwords, PIN numbers or One Time Pass codes.



delitosinformaticos@santander.com.ar



mensajesospechosoclientes@santander.com.co



fraudesinformaticos@santander.cl



phishing@gruposantander.es



csirt@santander.pl



delitosinformaticos@santander.com.uy



alerta fraudes@santander.pt



delitosinformaticos@santander.com.mx



reportabuse@santander.us



phishing@santander.co.uk



ciberseguridad@santander.com.pe



suspeita@santander.com.br

Impersonating another company

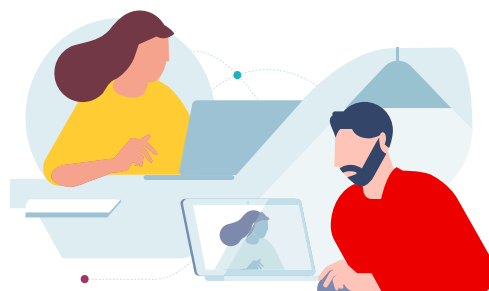
It's important you also let them know.

You can reach the impersonated company via their official channels, such as their website, telephone number or email address.

Never use the contact details included in the communication you have received.

Do the right thing

When you report you are helping others, as the affected companies will be able to investigate the cases and take action to prevent and stop similar attacks.



REMEMBER, IF YOU SUSPECT IT, REPORT IT.